IFW

PTO/SB/21 (09-04)

OIPE NOV 28 2005 PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 16

Application Number	10/804,618
Filing Date	March 18, 2004
First Named Inventor	Taguchi, Yuichi
Art Unit	2171
Examiner Name	Unassigned
Attorney Docket Number	16869B-102700US

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☒ Renewed Petition to Make Special
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):

Return Postcard

Remarks The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Townsend and Townsend and Crew LLP		
Signature			
Printed name	Chun-Pok Leung		
Date	November 23, 2005	Reg. No.	41,405

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature			
Typed or printed name	Joy Salvador	Date	November 23, 2005

PATENT
Attorney Docket No.: 16869B-102700US
Client Ref. No.: HAL295
(340400055US01)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

YUICHI TAGUCHI

Application No.: 10/804,618

Filed: March 18, 2004

For: MANAGEMENT METHOD FOR DATA RETENTION

Customer No.: 20350

Examiner: Unassigned

Technology Center/Art Unit: 2171

Confirmation No.: 7877

RENEWED PETITION TO MAKE SPECIAL FOR NEW APPLICATION UNDER M.P.E.P. § 708.02, VIII & 37 C.F.R. § 1.102(d)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Decision dated November 8, 2005 dismissing the original petition to make special, Applicants respectfully submit a renewed petition to make special the above-identified application under MPEP § 708.02, VIII & 37 C.F.R. § 1.102(d). The application has not received any examination by an Examiner.

(a) The Commissioner has previously been authorized to charge the petition fee of $130 under 37 C.F.R. § 1.17(i) and any other fees associated with this paper to Deposit Account 20-1430. 8/23/05

(b) All the claims are believed to be directed to a single invention. If the Office determines that all the claims presented are not obviously directed to a single invention, then Applicants will make an election without traverse as a prerequisite to the grant of special status.

(c) Pre-examination searches were made of U.S. issued patents, including a classification search and a foreign patent database search. The searches were performed on or around June 15, 2005, and were conducted by a professional search firm, Mattingly, Stanger Malur & Brundidge, P.C. The classification search covered Class 360 (subclasses 48, 49, 53, and 60), Class 707 (subclass 10), Class 709 (subclasses 223, 226, 245, and 246), Class 711 (subclasses 148 and 154), and Class 713 (subclasses 160, 161, 165, 200, and 201). Because of the large size of these subclasses, keywords were used to narrow of number of documents returned. The foreign patent database search was conducted using Espacenet database and Japanese patent database.

(d) The following references, copies of which were previously submitted, are deemed most closely related to the subject matter encompassed by the claims:

(1) U.S. Patent No. 5,369,532;

(2) U.S. Patent No. 5,576,903;

(3) U.S. Patent No. 6,446,176 B1;

(4) U.S. Patent No. 6,480,963 B1;

(5) U.S. Patent No. 6,535,967 B2;

(6) U.S. Patent Publication No. 2002/0065835 A1;

(7) U.S. Patent Publication No. 2002/0174306 A1;

(8) U.S. Patent Publication No. 2003/0115204 A1;

(9) U.S. Patent Publication No. 2004/0044863 A1; and

(10) Japanese Patent Publication No. JP 2004-062216.

(e) Set forth below is a detailed discussion of references which points out with particularity how the claimed subject matter is distinguishable over the references.

A. Claimed Embodiments of the Present Invention

The claimed embodiments relate to managing data stored in a storage system for data retention purposes. An administrator inserts data management rules into data files so

that data management policy can be commoditized across multiple services. The data management rule information is stored inside of the data file directly (or attached thereto). In one implementation, the data management rules are included in the header of the data file.

Independent claim 1 recites a storage system, comprising a host configured to receive a data file from a client, the host including a data management rule set program that is operable to associate a management rule to the data file received from the client; a first storage subsystem configured to receive and store the data file from the host, the storage system including a storage controller and a plurality of storage volumes; and a data protection server including a data protection management program that cooperates with the first storage subsystem to protect the data file stored in the first storage subsystem.

Independent claim 10 recites a management server provided in a storage system, the storage system including one or more hosts and one or more storage subsystems. The management server comprises a memory to store data; a processor to process data; a network interface to link with one or more computers of the storage system; and a first management program to attach a management rule to a data file to be stored in a storage subsystem of the storage system, the management rule relating to a retention period or relocation information of the data file. The data file and the management rule are stored in a storage volume of the storage subsystem.

Independent claim 13 recites a management server provided in a storage system, the storage system including one or more hosts and one or more storage subsystems. The management server comprises a memory to store data; a processor to process data; a network interface to link with one or more computers of the storage system; and a first management program operable to access a header of a data file and manage the data file according to a management rule inserted in the header, the management rule relating to a retention period or relocation instructions of the data file.

Independent claim 16 recites a method for managing a data file stored in a storage system, the storage system including one or more client, one or more hosts, one or more storage subsystems. The method comprises receiving a data file including a header and a data content; attaching a management rule to the data file; storing the data file and the management rule at a first storage location in a first storage subsystem, the management rule

relating to retention or relocation information of the data file; and notifying a management program about the data file.

One of the benefits that may be derived is that data management rules are into data files so that data management policy can be commoditized across multiple services. For example, a retention period rule for a data file can be shared by multiple servers.

B. Discussion of the References

1. U.S. Patent No. 5,369,532

The patent to Dodt et al., US 5369532, discloses a method and apparatus for managing data on rewritable media to define read/write operational status. Control software and hardware in the tape drive control unit creates and manages a header segment at the beginning of the magnetic tape 100. This header segment 105 includes an administrative information section that contains data relating to the magnetic tape itself. The administrative information 501 includes read/write status information such as the write protect status of the magnetic tape that enables the tape drive control unit 350 to manage the data records written onto the magnetic tape without reference to any other source of administrative data. In addition, each data record written on the magnetic tape includes a header which denotes the read/write status of the data record. The second section of the header segment includes administrative information including the file safe (write protect) status of the magnetic tape. The tape drive 300 operates independent of the host computer to ensure that the data records stored on this magnetic tape are not inadvertently overwritten by the host computer if this magnetic tape is designated as a file safe tape (see col. 13, line 62 to col. 14, line 19). This is accomplished by reading the administrative data to determine the file safe status of the magnetic tape. As a further level of security, each data record scan group that is written on to this rewritable media includes a header prepended thereto that includes file safe status bit to indicate whether this specific data record is write protected. See, e.g., Abstract and column 2, line 60-column 3, line 5.

The reference is directed to the use of administrative information that enables the tape drive control unit to manage the data records written onto the magnetic tape without reference to any other source of administrative data. The administrative information does not constitute a data management rule that is associated with a data file received the a client for

data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

2. U.S. Patent No. 5,576,903

The patent to Brown et al., US 5576903, discloses a method and apparatus for administering data on magnetic tape medium by way of a header segment. The control software and hardware in the tape drive control unit creates and manages a header segment at the beginning of the magnetic tape. This header is interposed between a leader portion of the magnetic tape on the 3480-type cartridge and the remainder of the magnetic tape contained therein. This header segment contains two sections, a first of which is a data record directory that is used by the control unit to denote the location of each data record written on to the magnetic tape as well as administrative information associated with the data record. The second section of the header is an administrative information section that contains data relating to the magnetic tape itself. The administrative information includes the identification of the tape volume, the tape drive, write protect status of the magnetic tape, identification of the media, error record log and other information that enables the user, the host processor and the tape drive control unit to manage the data records written onto the magnetic tape without reference to any other sources of administrative data. In addition, the header itself can be self protected by computing an error correction code across the data contained within the header to enable the control unit to identify whether the header integrity has been compromised. The internal leader header segment 105 of magnetic tape 100 is read on every load of magnetic tape cartridge 301 into a tape drive subsystem 300. The internal leader header segment 105 is updated by magnetic tape drive subsystem 300 prior to magnetic tape 100 being physically

unloaded therefrom in order to update the header information concerning read and write information contained therein. The internal leader header 105 illustrated in FIG. 5 includes two segments: administrative information 501, and data record search directory 502. The data record search directory 502 includes a plurality of entries, one for each search segment boundary that are crossed. See, e.g., Abstract and column 5, lines 40-51.

The reference is directed to the use of administrative information that enables the tape drive control unit to manage the data records written onto the magnetic tape without reference to any other source of administrative data. The administrative information does not constitute a data management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

3. U.S. Patent No. 6,446,176 B1

The patent to West et al., US 6446176, discloses a method and system for transferring data from a primary storage system 300 to a secondary storage system 302 in which the primary storage system includes primary storage volumes (304, 306, 308) and a primary bridge volume 316 and the secondary storage system includes secondary storage volumes (310, 312, 314) and a secondary bridge volume 320. A link between the primary bridge volume and the secondary bridge volume is established. The data to be transferred from a primary storage volume to a corresponding secondary storage volume is then copied onto the primary bridge volume by using pointers to the data of the primary storage volume (internal snapshot copy). Snapshot copied data is then transferred from the primary bridge volume to the secondary bridge volume over the link. The data is then moved from the

secondary bridge volume to the secondary storage volume corresponding to the primary storage volume to put the primary storage volume and the corresponding secondary storage volume in synchronization. This process enables the use of bridge volumes to handle data synchronization responsibilities in addition to data transferring responsibilities thereby allowing the host to not have to compete for access to primary storage volumes. In transferring tracks of data from a primary volume to a corresponding surrogate volume, the target volume is identified such that the data can be relocated to the correct volume once received at the secondary data bridge volume. The target volume is identified by incorporating a header with the data being transferred between bridge volumes across the data path. The header includes virtual track addresses which are used to relocate the data to the appropriate secondary storage volume once the data is received at the secondary bridge volume. See, e.g., Abstract and column 7, lines 52-61.

The reference discloses that a target volume is identified by incorporating a header with the data being transferred between bridge volumes across the data path. Although it discloses the use of virtual track addresses in the header to relocate the data to the appropriate secondary storage volume once the data is received at the secondary bridge volume, the virtual track addresses do not constitute a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

4. U.S. Patent No. 6,480,963 B1

The patent to Tachibana et al., US 6480963, discloses a network system with integrated security protection facilities. The system involves a transmission unit and a reception unit, which are coupled to each other via a network. In the transmission unit, a data management unit performs centralized management of source data that is stored in a plurality of storage units in a distributed manner. In response to a data transmission request from a terminal local to the transmission unit, a data collection unit collects requested data items from the data management unit. A security processor applies appropriate security protection processes to the collected data, depending on its data confidentiality level. An identification data attaching unit attaches identification data to the transmission data. This identification data informs the recipient of what sequence of security process primitives has been applied to the source data. A transmitter sends out the security-protected data over the network. In the reception unit, a receiver accepts the data sent from the transmission unit, and an identification data extracting unit extracts the identification data attached to the received data. With this identification data, an unprotection unit unprotects the received data, thereby reconstructing the original data contents. The header field 90 contains information indicative of what communication protocols are used and what type of data is enclosed in the packet. The source and destination address fields (91, 92) convey the names of the sender and recipient. The data name field 93 indicates the title of the security-protected data 96. See, e.g., Abstract and column 12, line 66 to column 13, line 7.

The reference is directed to an identification data for informing the recipient of a transmission data of what sequence of security process primitives has been applied to the source data. The identification data does not constitute a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation

instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

5. U.S. Patent No. 6,535,967 B2

The patent to Milillo et al., US 6535967, discloses a method and apparatus for transferring data from a first storage system to a second storage system in which the first storage system includes a first plurality of storage devices and the second storage system includes a second plurality of storage devices. Data is transferred using a pair of devices selected for transferring data for all of the storage devices. Data to be transferred from source storage devices within the first plurality of storage devices is placed or queued on a selected primary storage device within the first plurality of storage devices. The data is sent to a selected secondary storage device within the plurality of storage devices. In transferring tracks of data from a primary volume to a corresponding secondary volume, the target volume is identified such the data can be relocated to the correct volume once received at the secondary data bridge volume. The data is relocated from the selected secondary storage device to target storage devices within the second plurality of storage devices. The data in the payload may be compressed depending on the implementation. The header 402 includes a virtual track address (VTA) 406 and a bridge device number (BDN) 408. VTA is used to relocate the data to the appropriate volume once the data is received at the secondary data bridge volume. See, e.g., Abstract and column 6, line 56 to column 7, line 10.

The reference discloses the use of virtual track address to relocate data to the appropriate volume once the data is received at the secondary bridge volume. The virtual track address does not constitute a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file,

the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

6. U.S. Patent Publication No. 2002/0065835 A1

The published patent application of Fujisaki, US 20020065835, discloses a file system assigning a specific attribute to a file, a file management method assigning a specific attribute to a file, and a storage medium on which is recorded a program for managing files. In a file system configured by one or a plurality of volumes, policy attribute data is set in correspondence with the path information of a directory, and a file is managed based on the policy attribute data. As a result, a policy specific to the directory can be set while maintaining the compatibility with an existing file system. For example, a volume number is set as the policy attribute data of a file, so that a file system administrator can specify the storage location of the file. Attribute data to be processed, which is possessed by a parent directory, is obtained from metadata (information for managing data such as the attribute, contents, storage location, etc. of data) (step S14). The attribute data to be processed (policy attribute data), which is possessed by the registered policy data, is compared with the obtained data (step S15). Then, it is determined whether or not the attribute data of the parent directory is inherited according to the inheritance attribute defined for each attribute data (step S16). If it is determined that the attribute data of the parent directory is inherited, this data is assigned to the target directory (steps S17 and S18). If it is determined that the attribute data of the parent directory is not inherited, specified attribute data is assigned to the target directory (steps S19 and S18). See, e.g., Abstract; Fig. 3; and paragraph [0095].

The reference discloses the use of policy attribute data to manage a file. The policy attribute data does not constitute a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10;

managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

7. U.S. Patent Publication No. 2002/0174306 A1

The published patent application of Gajjar et al., US 20020174306, discloses a system and method for policy based storage provisioning and management. A storage provisioning policy is created by specifying storage heuristics for storage attributes using storage heuristic metadata. Storage attributes characterize a storage device and storage heuristic metadata describe how to specify a storage heuristic. Using the storage heuristic metadata, storage heuristics are defined to express a rule or constraint as a function of a storage attribute. In addition, the storage provisioning policy may also specify mapping rules for exporting the storage to a consumer of the storage, such as the server or server cluster. After storage provisioning policies are created, discovered data for storage attributes associated with the storage devices are compared to related storage heuristics for the storage attributes found in the storage profile. Then, one or more storage devices are selected for provisioning if the discovered attributes of the storage devices satisfy the storage heuristics in the storage profile. The storage that is provisioned may be any type of storage, such as storage units of storage devices, storage devices, and the like. In another embodiment, virtual media units may be created if no storage devices satisfy the storage heuristics in the storage profile. The selected or created storage units are then provisioned to the storage consumer using the mapping rules specified as part of the storage provisioning policy. See, e.g., Abstract and paragraphs [0006]-[0009] and [0031]-[0032].

The reference relates to the use of storage heuristic metadata to create a storage provisioning policy for specifying mapping rules. It does not, however, disclose a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a

data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

8. U.S. Patent Publication No. 2003/0115204 A1

The published patent application of Greenblatt et al., US 20030115204, discloses a system and a method for defining policies that can be used in various types of management applications for automating and performing one or more actions on at least one resource in a computer network environment. The system is configured to receive a signal indicating occurrence of a monitored event (step 302); identify rules having first conditions that are based upon the monitored event (step 304); and identify one or more rules from the rules having the first conditions for which the first conditions are satisfied (step 306). The one or more rules define one or more actions to be performed upon satisfying one or more second conditions based upon one or more non-monitored attributes of at least one resource. At least one rule is identified from the one or more rules for which the one or more second conditions of the at least one rule are also satisfied (step 308). The one or more actions to be performed for the at least one rule are defined, and are performed on the at least one resource. The one or more rules define one or more actions to be performed upon satisfying one or more second conditions based upon one or more non-monitored attributes of at least one resource. The method further comprises determining the one or more actions to be performed for the at least one rule, and performing the one or more actions on the at least one resource (step 310). See, e.g., Abstract; Fig. 3; and paragraphs [0011]-[0015] and [0070].

The reference discloses the use of rules and policies for automating and performing actions on resources in a computer network environment. It does not, however, disclose a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent

claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

9. U.S. Patent Publication No. 2004/0044863 A1

The published patent application of Trimmer et al., US 20040044863, discloses a method of importing a plurality of data from a physical data storage device into a virtual tape library system that is used with a data protection application. The virtual tape library system is usable with an existing data protection application designed for use with a physical tape library without modifying the existing data protection application. The method includes: triggering a signal representing a command to import the plurality of data from the physical data storage device; providing a controller that receives the signal; providing a data storage medium in communication with the controller, the data storage medium has at least one virtual library defined thereon; and copying at least a portion of the plurality of data from the physical data storage device to a virtual tape. When data from a physical data storage device is imported, it will preferably also have a physical label or barcode that matches the virtual barcode that was assigned by the data protection application. Thus, the virtual tape that is created and/or imported by the system 10 is identical to that contained on the physical data storage device 20. It is preferable that the virtual barcode be stored in the header extension of the meta data for each block of data on a data disk. See, e.g., Abstract and paragraph [0048].

The reference discloses a virtual barcode stored in the header extension of the meta data for each block of data on a data disk. The virtual barcode does not constitute a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1;

attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

10. Japanese Patent Publication No. JP 2004-062216

The Japanese patent document to Ishii, JP 2004062216, discloses a method and a system for data filing which classify and record a received data file according to attribute information on the data file while recording data according to a digital data management format rule. The method includes a data file attribute information readout step for reading attribute information of data files out, a data file classification step for setting the contents of the attribute information read out at the attribute information readout step as classification standards and classifying the data files into a plurality of groups according to the classification standards, and a collection information recording step for recording classification information according to classifications at the data file classification step as collection information separately from a specified file name of a specified directory recorded at a data file recording step.

The reference is directed to classifying and recording a received data file according to attribute information on the data file. The attribute information does not constitute a management rule that is associated with a data file received the a client for data protection or retention/relocation. The reference fails to teach associating a management rule to a data file received from a client, and storing the data file in a storage subsystem, the data file being protected by a data protection management program, as recited in independent claim 1; attaching a management rule which relates to a retention period or relocation information to a data file, wherein the data file and the management rule are stored in a storage volume of a storage subsystem, as recited in independent claim 10; managing a data file according to a management rule inserted in the header of the data file, the management rule relating to a retention period or relocation instructions of the data file, as recited in

independent claim 13; and attaching a management rule to a data file and storing the data file and the management rule in a storage subsystem, the management rule relating to retention or relocation information of the data file, as recited in independent claim 16.

(f) In view of this petition, the Examiner is respectfully requested to issue a first Office Action at an early date.

Respectfully submitted,

Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
RL:rl
60642866 v1